COMMANDERS DIGEST
VOL. 18, NO. 7/AUGUST 14, 1975

How the PRIVACY ACT Impacts on DoD

PRIVACY ACT

How the Privacy Act Impacts on the Department of Defense

This *Commanders Digest* concerns the Privacy Act of 1974 which was signed into law December 31, 1974, and is encoded in Title 5, United States Code, as Section 552a, immediately following the Freedom of Information Act.

Basically, the Privacy Act establishes in law a property right of individuals in information about themselves. In many ways, the Privacy Act complements rather than conflicts with the Freedom of Information Act.

The Privacy Act is applicable to records systems containing personal information—manual systems as well as automated systems—maintained by any Federal agency. The term "agency" includes any executive department, Military Department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Federal Government.

The act concerns *individual* humans—not corporations, institutions, and the like. This distinction was made to insure that the act left untouched the Federal Government's related activities for such purposes as economic regulations.

The act applies to U.S. citizens and aliens lawfully admitted for permanent residence.

For purposes of the act, a "record" may be any written or recorded data containing a single item of information or a large amount of information. For example, an individual personnel file is a record. And a file card with an individual's name and date of birth is also a record. The term "record" was defined by the Congress to assure the intent that a record can include as little as one descriptive item about an individual. By this definition, a record can be part of another record. Therefore, prohibitions on the disclosure of a record, for example, apply not only to the entire record in the conventional sense but also to any item or grouping of items from a record provided that such grouping includes an individual identifier.

By and large, however, the act is most concerned with systems of records. But again, a system of records may be as simple or as complex as suggested.

Ask yourself, "How do I gain access to a particular record?" If it is by an individual's name, a social security account number, or some other number assigned or associated with a particular individual, then the record system is probably subject to the act.

The Privacy Act of 1974 is based on these four principles:

- There should be no secret systems of records on individuals.
- There should be no unforeseen

uses or disclosures of information contained in records about individuals.

- Individuals should have access to records about themselves and be permitted to review their records, to make copies, and to file material to correct or dispute records they feel are inaccurate.
- Finally, records should contain no **unnecessary** or, insofar as possible, **inaccurate** information about individuals.

Consider how each of these principles is provided for in the act. To insure that there are no secret records maintained about individuals, the act requires that each agency publish in a public notice the existence of all systems of records subject to the act. These are systems of records containing information about individuals and accessible or retrieved by name or personal identifier such as an identifying number. The public notice — in the *Federal Register* — must contain:

- The *name* of the *system;*
- The *location* at which the system of records is maintained;
- The *types* of *people* on which the records are maintained;
- The *types* of *information*—in general terms—in each record;
- The *statutory authority* under which the records are maintained;
- The *routine uses* for the records and the information;
- The *policies* and *procedures* for managing the records, including the form for each record—such as, hard copy or computer tape;
- *Safeguards;*
- The *retention* and *disposal* procedures;
- The title and official address of the *system manager* and
- The *sources*—again, in general terms—of the information in each record.

The public notice must be published annually for each system of records, with the first public notice by August 27, 1975. Any modification of existing records, or any proposed new systems of records, must also be published in *the Federal Register* at least 30 days before implementation of the new system. In addition, agencies must notify the Congress and the Office of Management and Budget when modifying an existing system or establishing a new system of records.

Some records systems may be exempt from certain provisions of the Privacy Act, but no record system is exempt from certain minimum public notice requirements.

To eliminate unforeseen uses of information, the act requires that the public notice include all "*routine uses*" of information on an individual. The term "routine uses" should be interpreted as broadly as possible. The reason is that after the public notice and the act's effective date of September 27, 1975, no other uses or disclosures of personal information may be

"To insure that there are no secret records maintained about individuals, the act requires that each agency publish in a public notice the existence of all systems of records subject to the act."

"Avoid interpreting this (provision) as outlawing certain records . . . Rather, the preferred position should be, Do we need a particular system of records to accomplish our duties?"

made without the express written consent of the individual concerned—with violation subject to criminal prosecution.

Part of the requirement for individual approval of all disclosures is met in the public notice of routine uses. Insuring full compliance, however, will require attaching an explanation comparable to the public notice to any and all forms completed by an individual, when the forms or information from such forms become part of a record or system of records.

For any disclosure or use other than those identified under routine uses—or under one of the exemptions—it is necessary to seek and obtain the written approval of each individual concerned. Each record must carry an "audit trail," tracing all disclosures of the record, in whole or in part, whether made under routine uses or otherwise, outside the controlling agency.

These are the permitted disclosures:

A— within the agency to individuals needing the information in the performance of their duties.

B— disclosures required or permitted under the Freedom of Information Act.

C— for "routine uses" which have been published in *the Federal Register*.

D— to the Bureau of the Census for census or survey purposes.

E— for statistical purposes, provided the record or information is transferred in a form not individually identifiable.

F— to the National Archives for records of historical value, but not when the General Services Administration acts as a temporary repository for inactive records.

G— to another agency for civil or criminal law enforcement activity, if such activity is within the charter of the agency and on written request from the agency head.

H— to another person under compelling circumstances involving the health and safety of an individual.

I— to the Congress, Congressional committee, or subcommittee in pursuit of matters in its jurisdiction. However, this does not apply to individual Congressmen acting on behalf of a constituent in matters not falling under the jurisdiction of a Congressional committee or subcommittee.

J— to the Comptroller General on business of the General Accounting Office.

K— under a court order. However, if an agency is required to release records under court order, it must make a reasonable effort to notify the individual. And, before releasing information to someone outside the Government, a reasonable effort must be made to assure that the information is accurate, complete, timely, and relevant.

So that an individual may have access to any records maintained about him or her, it is necessary to include in public notice the means by which an individual may see, obtain copies of, and request corrections to any such records. The record must be provided for an individual's inspection in a form including copies which the individual can understand. There are some records to which individual access may seem inappropriate and the act provides for certain exemptions from this and other provisions of the act.

After an individual has gained access to his or her record (and if the person determines something is in error), that person may ask that the record be corrected. A request to amend a record must be responded to within 10 working days of receipt. The determination may be that correction is unwarranted. If no correction is made, the individual concerned may file an appeal according to published agency procedures; and review of the appeal must be completed within 30 working days. If the appeal is denied, the individual may file suit in Federal court and submit a statement for inclusion within the record in question.

If it is agreed to correct a record, it is also important to insure that the correct information is provided to any and all persons or activities or agencies to whom the erroneous record has been furnished prior to the correction. The "audit trail" helps here. The audit trail is required to be retained for five years or the life of the record, whichever is longer.

Information may be withheld to protect the confidentiality of an investigative source. Where it is possible to permit individual access to a record and the information in that record without divulging a confidential source, granting access is required. Confidentiality of a source may be implicit until the act's effective date of September 27, 1975. After that date, all guarantees of confidentiality must be explicit.

The act restricts record keeping to only those types of information needed to fulfill an express statutory purpose. It should be noted that there are certain "housekeeping" statutes which may be suitable, in the absence of specific statutes, dictating a given function or system of records. Obviously, one of the purposes of this provision of the act is to clear files of "nice to have" but otherwise unnecessary files or systems of records. Interpreting this as "outlawing" certain records, however, should be avoided. Rather, the preferred position should be, "Do we need a particular system of records to accomplish our duties?"

Restrictions have been placed on

use of the social security account numbers,—more on this later—and there are strict prohibitions from maintaining records of individual exercise of first amendment rights without the express permission of the individual concerned, or as provided by statute or for an authorized law enforcement activity. Again, portions of this provision are exempted, but only for specified purposes.

To avoid the need to make corrections, the act provides that agencies should obtain as much information as practicable directly from the individual. All of this is by way of satisfying the requirement that agencies maintain records used in making determinations with such accuracy, relevance, timeliness, and completeness as is reasonable to assure fairness to individuals.

The major portions and requirements of the Privacy Act do not become effective until September 27, 1975. However, the following provisions are in effect now.

There is in existence a Privacy Protection Study Commission. The Office of Management and Budget is the executive agency responsible for developing guidelines for agency implementations of the act.

Finally, no system of records established after January 1, 1975, may include an individual's social security number without express statutory provision. Our existing records systems, and additions to those systems, may still require the social security number.

There are both civil and criminal sanctions for violations of the Privacy Act. Civil suits may be founded on an agency refusal to amend a record on request by an individual, improper denial of individual access to a record, and/or failure to maintain a record accurately. Suit may be filed, against the agency or an officer of that agency for any failure to implement a provision of the act where such failure leads to an adverse determination against an individual.

If the plaintiff's suit is upheld, agencies can expect to be directed to take the necessary corrective actions and to pay the court costs and all lawyer's fees. In addition, where the litigant can show damage was done, an agency may be assessed damages at a minimum of $1,000. Suit must be filed within two years of the occurence of the violation of the act.

Criminal prosecution may be brought against individuals for willful unauthorized disclosure of a record or information in a record; failure to publish a notice of the existence of a system of records; and gaining access to a record under false pretenses. The violation is a misdemeanor and is subject to a fine of up to $5,000.

As mentioned earlier, the act authorizes exemptions for some records from certain provisions. These are not automatic and must be invoked by the head of the

COMMANDERS DIGEST

Vol. 18, No. 7, August, 14, 1975

A publication of the Department of Defense to provide official and professional information to commanders and key personnel on matters related to Defense policies, programs and interests, and to create better understanding and teamwork within the Department of Defense.

Published weekly by the American Forces Press Service, 1117 N. 19th St., Arlington, Va. 22209, a unified activity of the Office of Information for the Armed Forces, OASD (M&RA). Reproduction of content is authorized.

Telephone: (202) OXford 4-5070
Autovon 224-5070

agency—normally the Secretary. This, however, does not relieve agencies from the requirement for the public notice of the existence of the system, and the exemption and the reasons therefor must be specified in *the Federal Register*. Exemptions may be either general or specific. There are two general exemptions: records of the Central Intelligence Agency; and those records maintained for law enforcement purposes by law enforcement agencies.

These are the seven specific exemptions:

A— classified information which is exempt from release under the Freedom of Information Act.

B— investigatory material compiled for law enforcement purposes, but beyond the scope of the general exemption covered previously.

C— records maintained in connection with providing protective service to the President and others under Title 18, United States Code, Section 3056.

D— records required by statute to be maintained and used solely as statistical records.

E— investigatory material compiled solely to determine suitability, eligibility, or qualification for Federal employment or Military Service, but only to the extent that disclosure would reveal the identity of a confidential source.

F— testing and examination material used to determine individual qualification for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process.

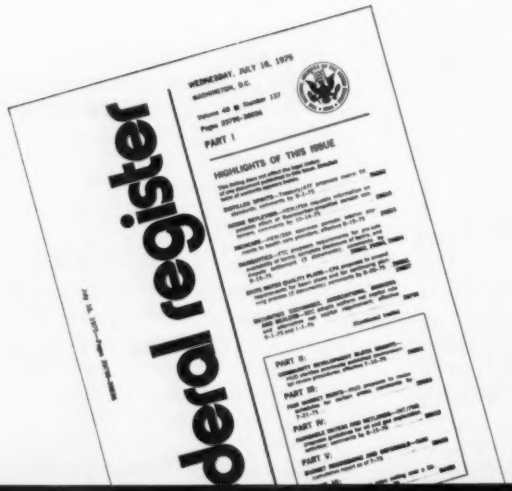
G— and finally, evaluation material used to determine potential for promotion in the Armed Services, but only to the extent that the disclosure of such material would reveal the identity of a source.

To implement the act in a uniform and consistent manner and on schedule, a structure has been established for the flow of information. Earlier the Office of Management and Budget responsibilities were discussed. On April 8, 1975 the Deputy Secretary of Defense, William P. Clements, Jr., announced the establishment of the Defense Privacy Board. The board was created primarily to insure that the act is implemented uniformly and on schedule throughout the Department of Defense. It will review all input from the Defense components for *the Federal Register* notices to insure consistency and uniformity and compliance with the requirements of the act.

The Defense Privacy Board will be responsible for submitting *Federal Register* notices for all Defense agencies to *the Federal Register*.

Service Privacy Act committees were established to function essentially the same for the Services as the Defense Privacy Board is functioning for the

"Criminal prosecution may be brought against individuals for willful unauthorized disclosure of a record or information in a record; failure to publish a notice of the existence of a system of records; and gaining access to a record under false pretenses. The violation is a misdemeanor and is subject to a fine of up to $5,000."



> ***"The Defense Privacy Board . . . will review all input from the Defense components for the*** Federal Register ***notices to insure consistency and uniformity and compliance with the requirements of the act."***

Department of Defense.

There are a number of tasks which face all executive agencies. All records subject to the act must be identified. This includes headquarters, major commands, bases, wherever records are maintained. All unnecessary records should be eliminated if they cannot be justified. Perhaps the best guide here is to answer this question: "Is this system of records important enough to our mission to justify the work of preparing the public notice, maintaining the disclosure audit trail, and meeting all other requirements of the act?" If the answer is not "yes," then eliminating the record system should be considered.

It is necessary to determine all exemptions and to publish the required public notice in *the Federal Register*. Of some importance is the need to list all "routine uses" of the record system. Include all potential uses under "routine" since failure to do so may lead to the need to contact the individual for permission to use the record for the intended purpose, or generate a "modification" announcement to be published in *the Federal Register* before the record could be released.

Service headquarters staff offices will be asked to identify and prepare the record system descriptions for publication in *the Federal Register* for all records prescribed by departmental directives, such as regulations, manuals, or other publications. Offices will also identify all systems of records maintained by every office within the headquarters. Major commands and separate operating agencies will identify and prepare descriptions of records systems which are prescribed by or unique to the commands at all levels.

Additionally, Service headquarters must develop training and information programs for all Military personnel. The Civil Service Commission will do the same for all civilian employees in the Federal Government. Appropriate notices to accompany forms which are used to collect personal information from individuals, such as the DD Form 398, Statement of Personal History, must also be developed. Ultimately, the notification required by the act will be incorporated in or attached to all affected forms as they are updated.

Throughout this whole process, all activities must maintain the records necessary for the first annual report due to the Congress on June 30, 1976. In that connection, managers should keep a record of costs incurred in implementing the act. Department of Defense Instruction 5000.22 should be used in developing cost figures.

Service headquarters will continue to provide updated guidance to their commands as it is received.

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
Subscription Price: $18.75 domestic per year; $4.70 additional for foreign mailing; 40 cents per single copy.
☆ U.S. GOVERNMENT PRINTING OFFICE 211-337/T-8